(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
18 August 2005 (18.08.2005)

PCT

(10) International Publication Number
WO 2005/076518 A1

(51) International Patent Classification[7]: H04L 9/08

(21) International Application Number:
PCT/JP2005/002514

(22) International Filing Date: 10 February 2005 (10.02.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

2004-033352	10 February 2004 (10.02.2004)	JP
2004-033355	10 February 2004 (10.02.2004)	JP
2004-169001	7 June 2004 (07.06.2004)	JP

(71) Applicant *(for all designated States except US)*: **NTT COMMUNICATIONS CORPORATION** [JP/JP]; 1-6, Uchisaiwai-cho 1-chome, Chiyoda-ku, Tokyo 100-8019 (JP).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **KAGAYA, Makoto. OGIHARA, Toshihiko. NOMURA, Susumu.**

(74) Agents: **MIYOSHI, Hidekazu** et al.; Toranomon Kotohira Tower, 2-8, Toranomon 1-chome, Minato-ku, Tokyo 1050001 (JP).

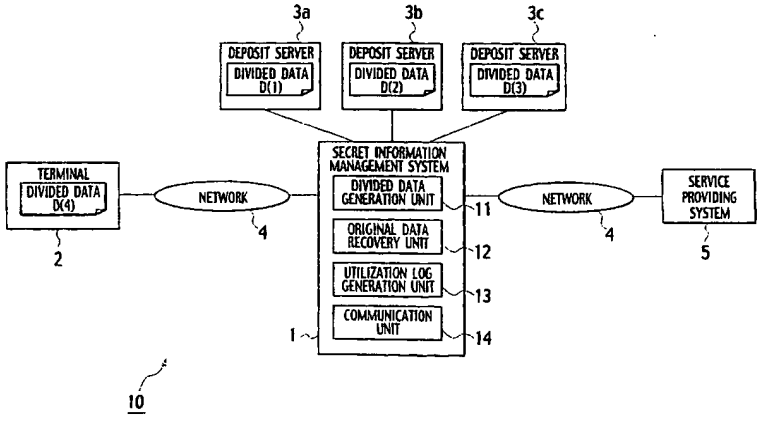
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SECRET INFORMATION MANAGEMENT SCHEME BASED ON SECRET SHARING SCHEME



(57) Abstract: In a secret information management system for managing a secret information of a user, the secret information is divided into a plurality of divided data by using a secret sharing scheme, such that the secret information can be recovered from a prescribed number of the divided data, and a part of the plurality of divided data is stored into a terminal of the user as user's divided data while a rest of the plurality of divided data are stored into one or more of deposit servers. Then, a plurality of re-divided data different from the plurality of divided data are generated, from a combination of the prescribed number of the divided data among the divided data stored in the deposit servers by using the secret sharing scheme, and a part of the plurality of re-divided data is stored into the terminal as newly generated user's divided data while a rest of the plurality of re-divided data are stored into the deposit servers as newly generated divided data.

WO 2005/076518 A1